UNIVERSITY OF JOHANNESBURG

FACULTY OF SCIENCE

ACADEMY OF COMPUTER SCIENCE AND SOFTWARE ENGINEERING

MODULE	IT00280/IT00299/IT28X80/IT8X299
	INFORMATION SECURITY GOVERNANCE
CAMPUS	APK
EXAM	NOVEMBER 2014

DATE: 2014/10/31 **SESSION:** 8:30 – 10:30

ASSESSOR(S) Prof SH von Solms

INTERNAL MODERATOR

EXTERNAL MODERATOR Dr J van der Merwe (DVT)

DURATION: 2 Hours **MARKS:** 100

THIS PAPER CONSISTS OF 3 PAGES INCLUDING THE COVER PAGE

INSTRUCTIONS:

1. Answer **ALL** the questions
2. Read the questions thoroughly
3. Write neatly and legibly
4. Ensure that all questions are clearly marked on the answer sheet.

REQUIREMENTS: NONE

QUESTION 1

You receive the following memo from the Chief Executive Officer of your company:

'*Last week I attended a seminar on Information Security Governance (ISG). One of the speakers referred to two documents she called COBIT 5 and ISO 27002. She specifically emphasized the value in using these two documents together in a company.*
Both these documents are known in our company, but we never thought of using them in a complementary mode for Information Security Governance (ISG) and Information Technology Governance (ITG).

Please provide me with a 3 page document on the following aspects, divided into corresponding sections:

1. *A brief explanation of Cobit 5 including its history, structure and what it should be used for.*
2. *A brief explanation of ISO 27002 including its history, structure and what it can be used for.*
3. *A comprehensive plan of how we can use these two documents together (complementary) for ISG and ITG in our company.*
   As this part of the report is the most important, I want you to spend the most of your report on this aspect.

   Please discuss

   3.1 *How we can use the 2 documents in a complementary mode for ISG. Be specific and provide a Plan of Action of how you will integrate them. This must be the core element of your report.*
   3.2 *How we can get certified if we use ISO 27002.*

As I intend to submit your report to the Board, please ensure that the document is logical, well structured, easy to follow and covers all the aspects I mentioned above.'

Write this document requested by the CEO.
Hint : For 3.1 above you will do well in referencing and using the 4 scenarios discussed in the paper 'Information Security Governance : Cobit or ISO 17799 or both?' which appeared in Computers and Security in 2005, and which is included in your study material – remember ISO 17799 is now ISO 27002.

Marks will be assigned as follows for the different aspects mentioned in the CEO's memo:

[50]

QUESTION 2

The education, training and awareness of end-users form an important component towards effective Information Security Governance.

2.1 The Conscious Competence Learning Model can play an important role in this regard. Name and briefly describe each of the four stages of this model. [8]

2.2 Explain comprehensively HOW you will use this Model if you have to create an Awareness Program for your company. Discuss what you will do to ensure that a novice user goes through all these stages. [12]

(Marks will be assigned for structure and readability). [5]

[25]

QUESTION 3

Discuss each of the following statements critically, ie indicate whether the statement is correct or wrong, and comprehensively motivate your answer in every case.

3.1 'Information Security Governance is purely a technical matter and should completely reside in the IT Department.'

3.2 'A statement in an Information Security Policy which cannot be measured is not worth the paper it is written on'.

3.3 'If every person in a company is Information Security Aware we do not need Information Security Policies and procedures.'

(3 x 7)

4 marks will be assigned for general presentation of 3.1 to 3.3.

TOTAL: [100]